ITS and Resilience – An ITS Nationals workshop

October 2020

The Network of National ITS Associations held a workshop dedicated to ITS and Resilience. This document summarises the event and includes the **Ten Features of a Resilient Transport Network in 2025** compiled and recommended by the workshop attendees.

These national associations contributed to the workshop:

ITS (UK), ITS Switzerland and ITS Germany – in the lead
ITS Estonia
ITS Ireland
ITS Romania
ITS&S Czech Republic

Also contributing: Cities Forum, ERTICO, Ifsttar, ISG Systems AB, Lagan, LOGMA Consulting, Simplifai Systems Limited, TELENAVIS SA, Triple Sign System AB, Turkish Ministry of Transport and Infrastructure

ITS Germany set the scene with a useful slide set:

ITS and Resilience
Setting the Scene From a German Perspective

Dr. Claus Habiger
ITS Germany

What is resilience?

Safeguarding (of critical infrastructures) against failure

- **Responsible in Germany: Federal Ministry of the Interior; BMI)**
  - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Federal Office for Civil Protection and Disaster Assistance)
  - Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)

Sectors to be considered (source: BMI; www.kritis.bund.de)

- **Health**
- **State and Administration**
- **Media and Culture**
- **Food**
- **Finance and Insurance**
- **Water**
- **IT and Telecommunications**
- **Traffic and Transport**

Changing Perspectives on Resilience

Traditionally Considered Scenarios

- **Natural Disaster**
- **State of Defence (War)**
- **Sabotage; physical**

New Framework

- **Scenarios have been widened**
  - Asymmetrical warfare
  - Terrorism
  - Non-physical attacks
- **Digitalisation opens up new possibilities**
- **Infrastructure connected via the internet**

What has ITS to do with this?

Two sectors of the Critical Infrastructure are involved

- **IT and Telecommunications**
- **Transport and Traffic**

Threats to be considered (source: BMI; www.kritis.bund.de)

- **Natural Threats**
  - Storms and tornados
  - Heavy rain and flooding
  - Droughts
  - Earthquakes
  - Pandemics
- **Accidents**
- **System failure**
- **Terrorism**
- **War**

Questions to be asked

What can ITS do to ease the threats

- **Accidents**
- **Pandemics**
- **etc.**

What does ITS add to the threats

- **System failure**
- **Terrorism**
- **etc.**

www.kritis.bund.de

What are the Feature of a resilient transport network?

- **What are the main ITS enablers?**
- **Which inter-dependencies do exist?**

Ten features of a resilient transport network in 2025

Feature	ITS Enablers	Notes
1 Always provides sufficient capacity for essential use by people and freight	• Control systems • Monitoring • Access controls and demand management • Incident and hazard management	*The importance of Standards* *We can never be risk free, so be clear in advance about priorities when the network is compromised*
2 Offers reliable and full coverage connectivity	• C-ITS • All forms of comms technologies used appropriately and as part of an agreed architecture	*This is the backbone of all ITS.* *We need to get better at pre-planning and future proofing our connectivity.* *A Europe wide Alternative Comms System, a short-term service for disaster comms & control, could be desirable.* *We need to differentiate Core Functionalities from Peripheral Operations which we can cope without in short term. Importance of having a clear view of which is which.* *This has to be integrated into the European Dataspace for Mobility as advocated by the European Commission*
3 Is protected against and offering quick recovery from natural incidents – weather, earthquake, wildfires, etc	• Monitoring systems (eg water levels, soil saturation, snow condition) feeding data into ITS services • Predictive information systems (meteorological, earthquake) feeding data into ITS services • The ITS equipment itself must be resilient to damage • ITS should be part of pre-agreed recovery plans • Asset management and automated direction of equipment including prior to incidents • Information and guidance to those using the networks	*ITS can help shorten the recovery period.* *The strategy changes, and ITS can help making appropriate strategy changes.* *Recover the most important aspects first. Somehow without knowing exactly what the main problems are. ITS gathers information which can be used to support strategic changes, including stopping activity which is not actually useful.* *Store equipment needed for major incident recovery. Example of relocation of snow ploughs in the US from north to south to help clear rubble from quakes / hurricanes. Example from Europe re forest fire equipment. "five things to keep in storage to help with major incidents"* *We must educate all subsidiarity levels that ITS is a Critical Infrastructure and assist the recovery*
4 Data rich, enabling excellent quality monitoring,	• Sensing and monitoring	*Data legislation* *Citizen acceptance*

intervention, prediction and planning	• Modelling including predictive • Open data principles with agreed standard formats • Workarounds based on available data • Enabling a wide range of useful ITS services	*Security and integrity*
5 Fully interoperable with ease of moving between modes and networks for people and for freight	• Information, planning, and booking services – MaaS style concept • e-Freight services • Secure series of transactions – blockchain style concept	*MaaS: connecting all modes in an equally usable way (data availability, quality, connectivity, standardisation)*
6 Secure against traditional crime, cyber crime, and terrorism	• Monitoring and identifying technologies • Physical and virtual security systems – hardened systems • Resilient to attach – ability to shut down partially but still operate pre-agreed core functions	*Dynamic risk analysis is always essential* *ITS systems are more "closed" than many others which makes them easier to secure* *Automation lacks the problem of legacy systems and should in principle be easier to keep secure because of this.*
7 Safe from crashes and accidents	• Information, warning and advice systems • Enforcement technology • Automation	*NB Automation will cause new safety hazards which will need to be managed*
8 Supports the resilience of its hinterland	• Supporting systems both of evacuation and of getting essential people, equipment and supplies into an area • Supports appropriate movements around major events	*Specialised, digital maps might be required (drop-off zones, alternative routes, etc.)*
9 Effective and reliable across borders	• Systems to assist users and freight pass across borders and in and out of ports in a timely but secure and compliant way	*Including special circumstances such as a pandemic or a specific security situation*
10 Always learning and improving	• Data – good quality, timely, affordable and easily reusable	Strategic objectives to be set by politics .

	• Modelling • Stream of new applications	

Suggested follow-on Network activities:

- **Guidance for building resilience into procurement**
- **Looking at resilience in comms systems and how this fits with the European Dataspace for Mobility**
- **Guidance for including ITS in pre-agreed recovery plans**
- **Consider how resilience can be built into data legislation**
- **Educate other organisations about that ITS is in fact a critical infrastructure**